Practical Attacks on a Class of Secret Image Sharing Schemes: Few Open Issues

Avishek Adhikari

Professor and Head Department of Mathematics
Presidency University
86/1 College Street, Kolkata 700073
E-mail : avishek.maths@presiuniv.ac.in

Abstract

Due to the enormous scientific progress of internet-related technologies, in today's scenario, it is very easy and cost-effective to transmit images over the internet or store them in cloud storage. However, transmitting or storing the images online does not appear to be 100% secure. That is why, sometimes, these are handy to the adversary or attacker to steal or destroy important images that are transmitted or stored digitally. It is very essential to protect these important images from being stolen or destroyed by means of hackers in certain fields, especially in industrial or defense sectors. To address these inconveniences, researchers have tried to develop numerous protection techniques together with cryptography. Secret Sharing (SS), one of the foremost very essential topics in cryptography, is considered to be one of the major primitives to protect important images. Secret Sharing is a method of sharing secret information among a set $\mathcal{P}$ of n persons in such a way that certain predefined sets of qualified participants can reconstruct the secret information while certain predefined forbidden sets of participants will have no information about the secret even if they come together. Due to its applications in Multiparty Computations, Private Information Retrieval, Private Distributed Storage, etc. secret sharing has become a pivot in research in information sciences. As a very particular case, if the secret is an image, then a secret sharing scheme is called a secret image sharing scheme. Broadly speaking, in the literature, Secret Image Sharing (SIS) schemes have two different approaches, one is visual cryptography and the other is Polynomial Based Secret Image Sharing. The basic security model of SIS guarantees that even with the knowledge of a non-qualified set of shares, an adversary is unable to guess the secret pixel. However, to capture more realistic scenarios, *active* attacks on the system must be considered – where an adversary controlling a non-qualified subset of shares may tamper with the shares and submit them during the reconstruction phase. Depending on the behavior, adversaries are broadly classified into two categories - *non-rushing* and *rushing*. In the former, an adversary does not wait for other honest participants to submit their shares and modify the adversarial share(s) without depending on the honest shares. Whereas, in the latter, the adversary waits to see the honest shares and then *rushes* to submit the corrupted share(s). Securing a system against such adversarial attacks is the ultimate goal of a secret image-sharing scheme. To model a realistic attack scenario we consider rushing adversary for examining the security of the existing polynomial-based SIS against such active attacks. In this talk, I shall mainly emphasize on few attacks on Secret Image Sharing Schemes.

References

[1] Adhikari, M. R. and Adhikari, A. (2014). Basic Modern Algebra with Applications. *Springer, New Delhi*, 978-81-322-1598-1.

[2] Adhikari, A. (2014). Linear Algebraic Techniques to Construct Monochrome Visual Cryptographic Schemes for General Access Structure and Its Applications to Color Images. *Designs, Codes and Cryptography*, 73(3):865–895.

[3] Dutta, S., Adhikari, A., and Ruj, S. (2018). Maximal Contrast Color Visual Secret Sharing Schemes. *Designs, Codes and Cryptography.*

[4] Dutta, S., Rohit, R. S., and Adhikari, A. (2016). Constructions and Analysis of Some Efficient $t-(k,n)^*$-visual Cryptographic Schemes using Linear Algebraic Techniques. *Des. Codes Cryptography*, 80:165–196.

[5] Sardar, M. K. and Adhikari, A. (2020a). A New Lossless Secret Color Image Sharing Scheme with Small Shadow Size. *Journal of Visual Communication and Image Representation*, page 102768.

[6] Naor, M. and Shamir, A. (1995). Visual cryptography. In De Santis, A., editor, *Advances in Cryptology — EUROCRYPT'94*, pages 1–12, Berlin, Heidelberg. Springer Berlin Heidelberg.

[7] Blakley, G. R. (1979). Safeguarding Cryptographic Keys. In *Managing Requirements Knowledge, International Workshop on(AFIPS)*, volume 48, page 313.